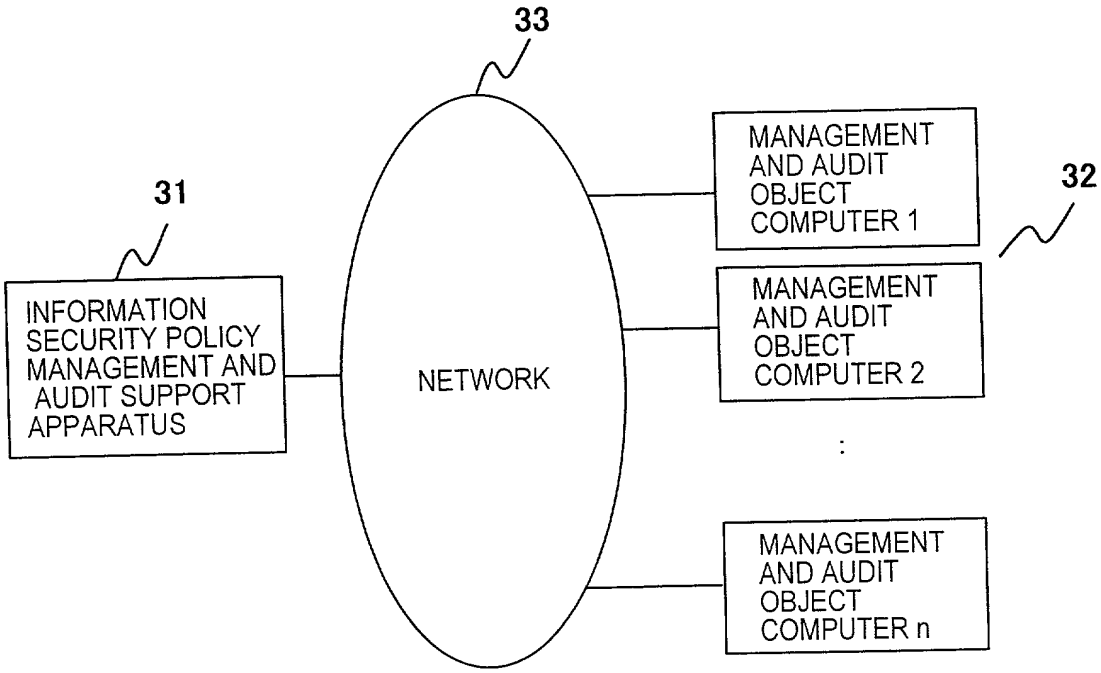
FIG.1


33
31
32
INFORMATION SECURITY POLICY MANAGEMENT AND AUDIT SUPPORT APPARATUS
NETWORK
MANAGEMENT AND AUDIT OBJECT COMPUTER 1
MANAGEMENT AND AUDIT OBJECT COMPUTER 2
:
MANAGEMENT AND AUDIT OBJECT COMPUTER n

T08T50" 2h7T9760

FIG.2

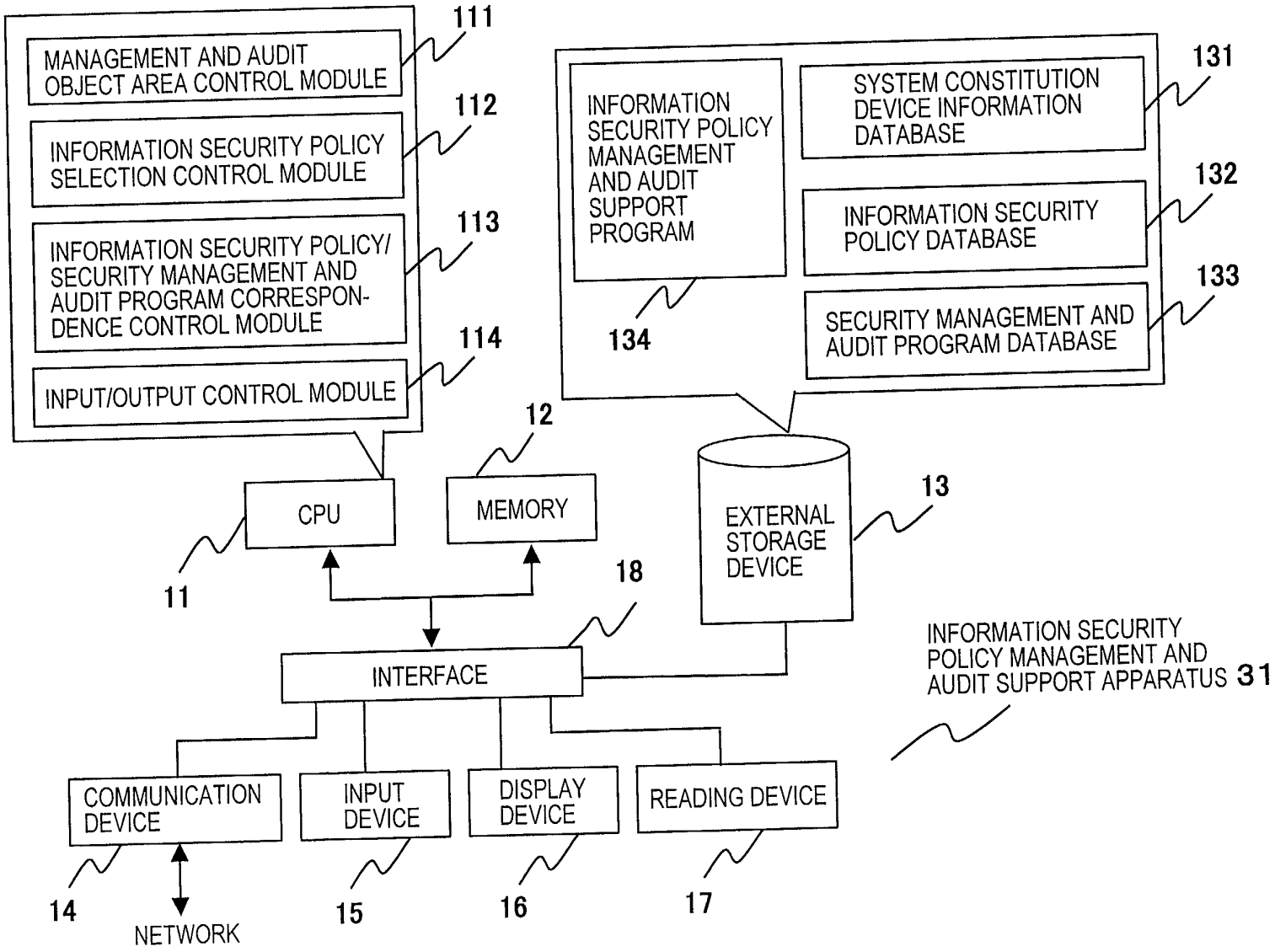


FIG.3

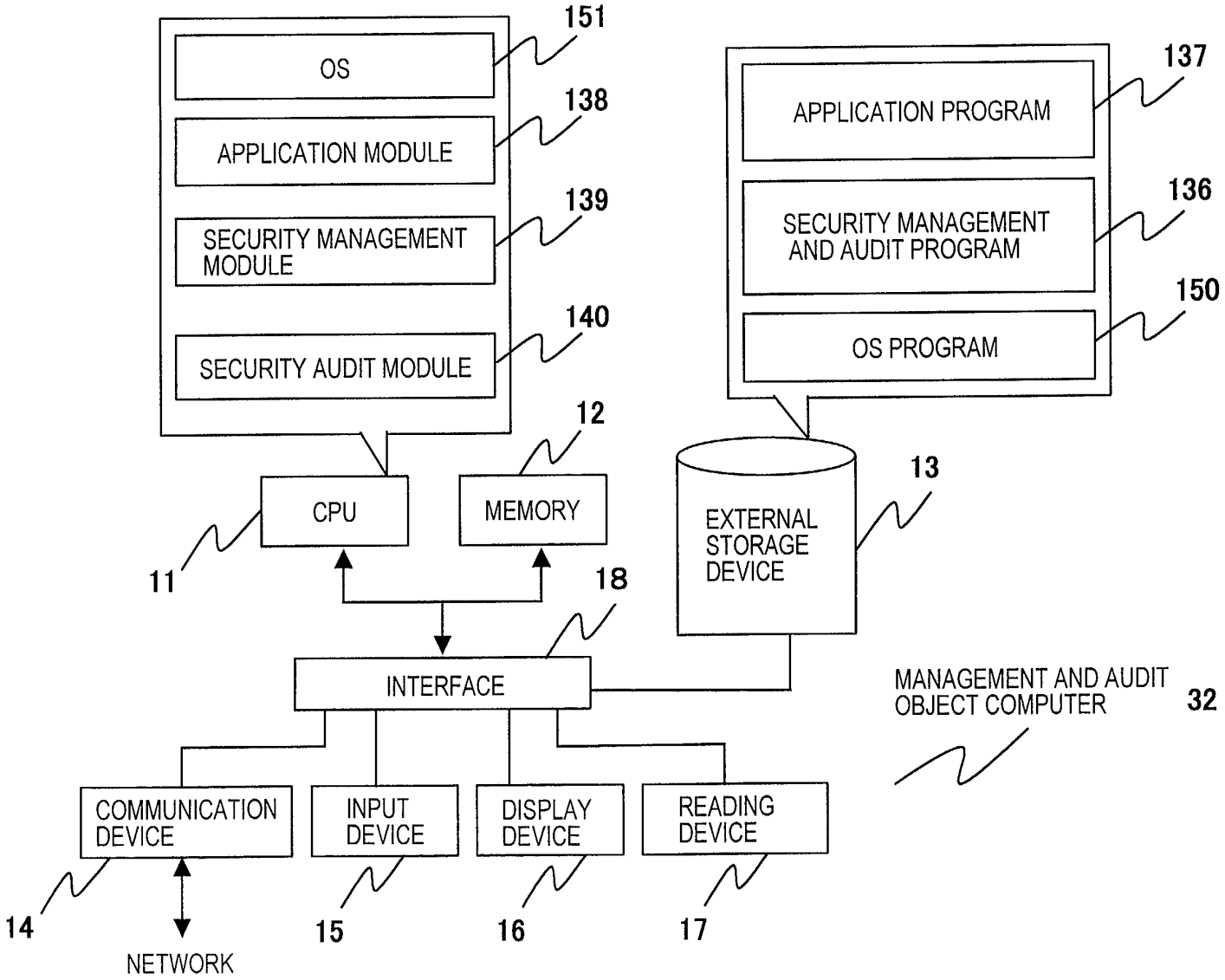

151
OS
138
APPLICATION MODULE
139
SECURITY MANAGEMENT MODULE
140
SECURITY AUDIT MODULE
137
APPLICATION PROGRAM
136
SECURITY MANAGEMENT AND AUDIT PROGRAM
150
OS PROGRAM
12
CPU
MEMORY
11
13
EXTERNAL STORAGE DEVICE
18
INTERFACE
MANAGEMENT AND AUDIT OBJECT COMPUTER
32
COMMUNICATION DEVICE
INPUT DEVICE
DISPLAY DEVICE
READING DEVICE
14
15
16
17
NETWORK

FIG.4

41 SYSID	42 APPARATUS CATEGORY	43 SOFTWARE CATEGORY	44 PROGRAM NAME	45 SELECTION POSSIBILITY
R001-00-01	ROUTER	—	A	YES
R001-00-02			B	NO
: :	: :	: :	: :	: :
S001-OS-01	SERVER	OS	H	YES
S001-OS-02			I	NO
S001-WEB-01		Web	X	YES
S001-WEB-02			Y	NO
S001-WEB-03			Z	NO
S001-MAIL-01		MAIL	O	YES
S001-DB-01		DATABASE	P	YES
: :	: :	: :	: :	: :

09751452-050104

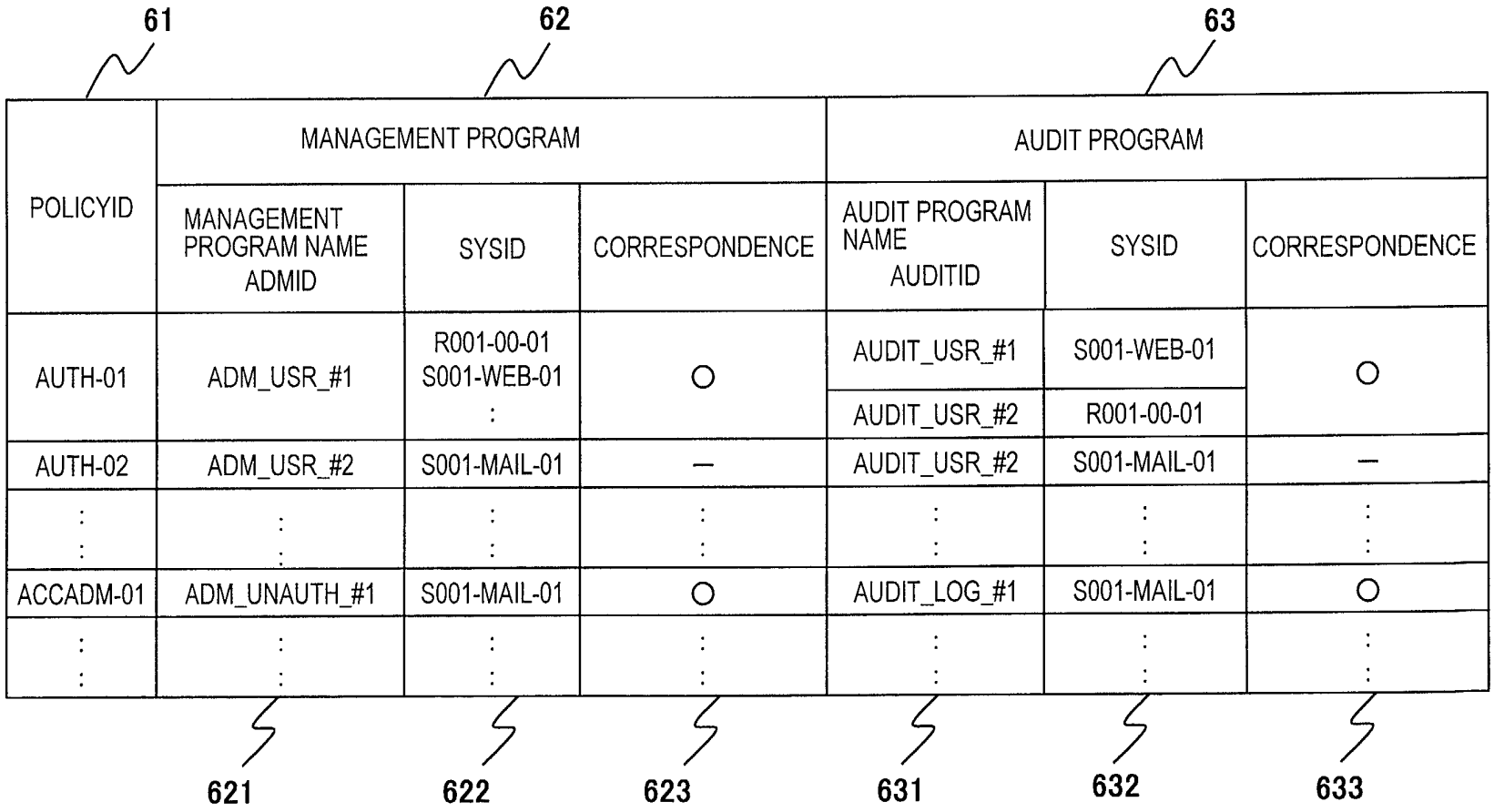
T08T50" 2h2T9260

FIG.5

51 POLICYID	52 MEASURE CATEGORY	53 SECURITY MEASURE	54 SELECTION POSSIBILITY
AUTH-01	IDENTIFICATION AND AUTHENTICATION FUNCTIONS	LIMITATION OF TERMINAL CAPABLE OF ACCESSING TO NETWORK	YES
AUTH-02	IDENTIFICATION AND AUTHENTICATION FUNCTIONS	EXECUTION OF GOOD PASSWORD SETTING FOR IDENTIFICATION AND AUTHENTICATION INFORMATION	YES
:	:	:	:
ACC-01	ACCESS CONTROL FUNCTION	LIMITATION OF COMMAND AVAILABLE FOR EACH TERMINAL AND USER	YES
ACC-02	ACCESS CONTROL FUNCTION	SETTING AND CHANGE OF AUTHORITY AND LIMITATION OF OPERATOR CAPABLE OF DELETING	YES
ACCADM-01	ACCESS OBSERVATION	EXECUTION OF DETECTION FOR FALSIFICATION OF DATA AND PROGRAM	YES
ACCADM-02	ACCESS OBSERVATION	RECORD OF COMMAND USED BY USER	NO
ACCADM-03	ACCESS OBSERVATION	ACQUIREMENT OF ACCESS LOG	NO
VIRUS-01	ANTI-VIRUS MEASURE	INSTALLATION OF VACCINE SOFTWARE	
VIRUS-02	ANTI-VIRUS MEASURE	PERIODIC VIRUS CHECK	YES
VIRUS-03	ANTI-VIRUS MEASURE	PERIODIC UPDATE OF VIRUS DEFINITION DATA	YES
:	:	:	:

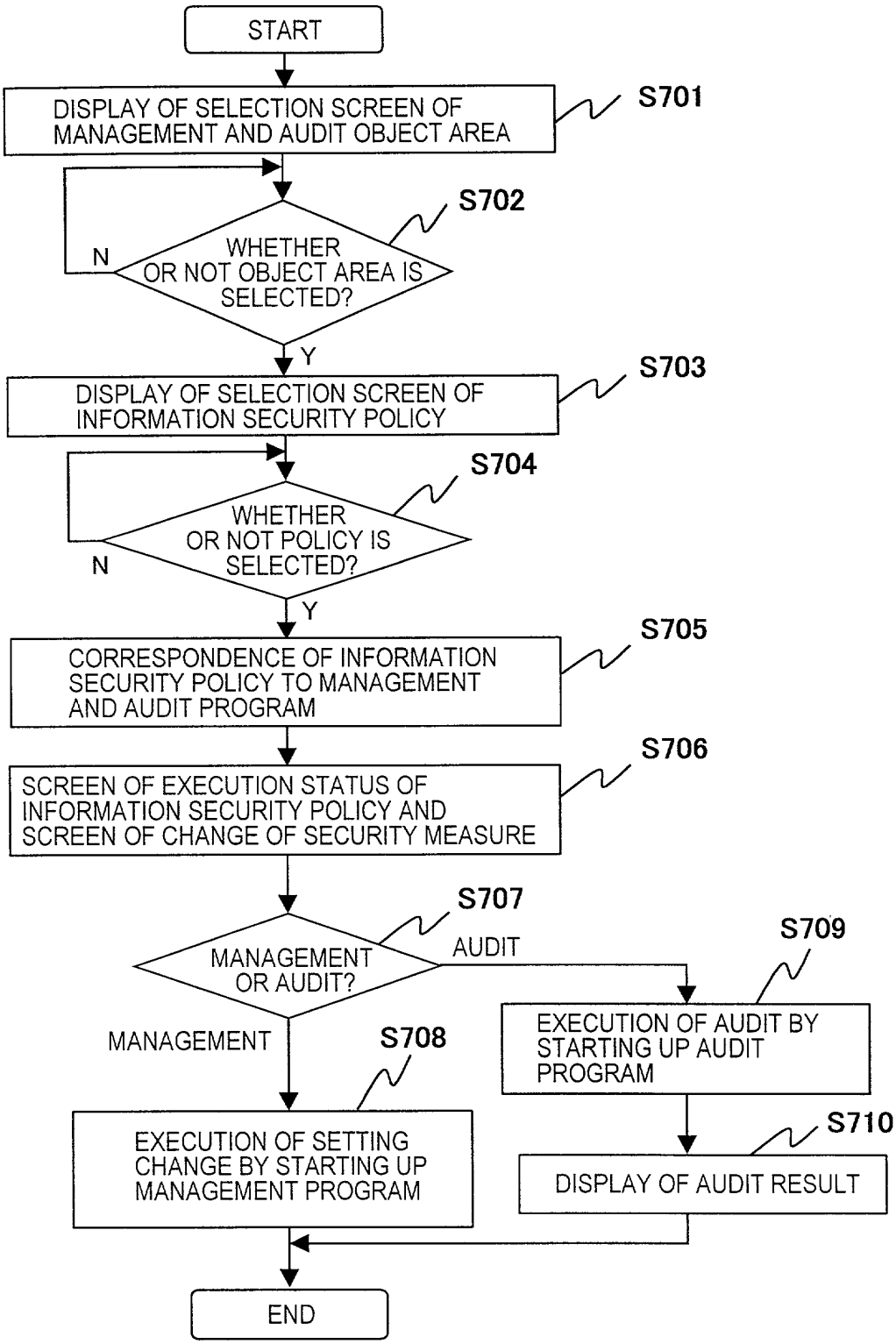
TOBTSO" 2h2T9260

FIG.6



POLICYID	MANAGEMENT PROGRAM			AUDIT PROGRAM		
	MANAGEMENT PROGRAM NAME ADMID	SYSID	CORRESPONDENCE	AUDIT PROGRAM NAME AUDITID	SYSID	CORRESPONDENCE
AUTH-01	ADM_USR_#1	R001-00-01 S001-WEB-01 :	○	AUDIT_USR_#1	S001-WEB-01	○
				AUDIT_USR_#2	R001-00-01	
AUTH-02	ADM_USR_#2	S001-MAIL-01	—	AUDIT_USR_#2	S001-MAIL-01	—
:	:	:	:	:	:	:
ACCADM-01	ADM_UNAUTH_#1	S001-MAIL-01	○	AUDIT_LOG_#1	S001-MAIL-01	○
:	:	:	:	:	:	:

FIG.7



09761742 - 051801

FIG.8

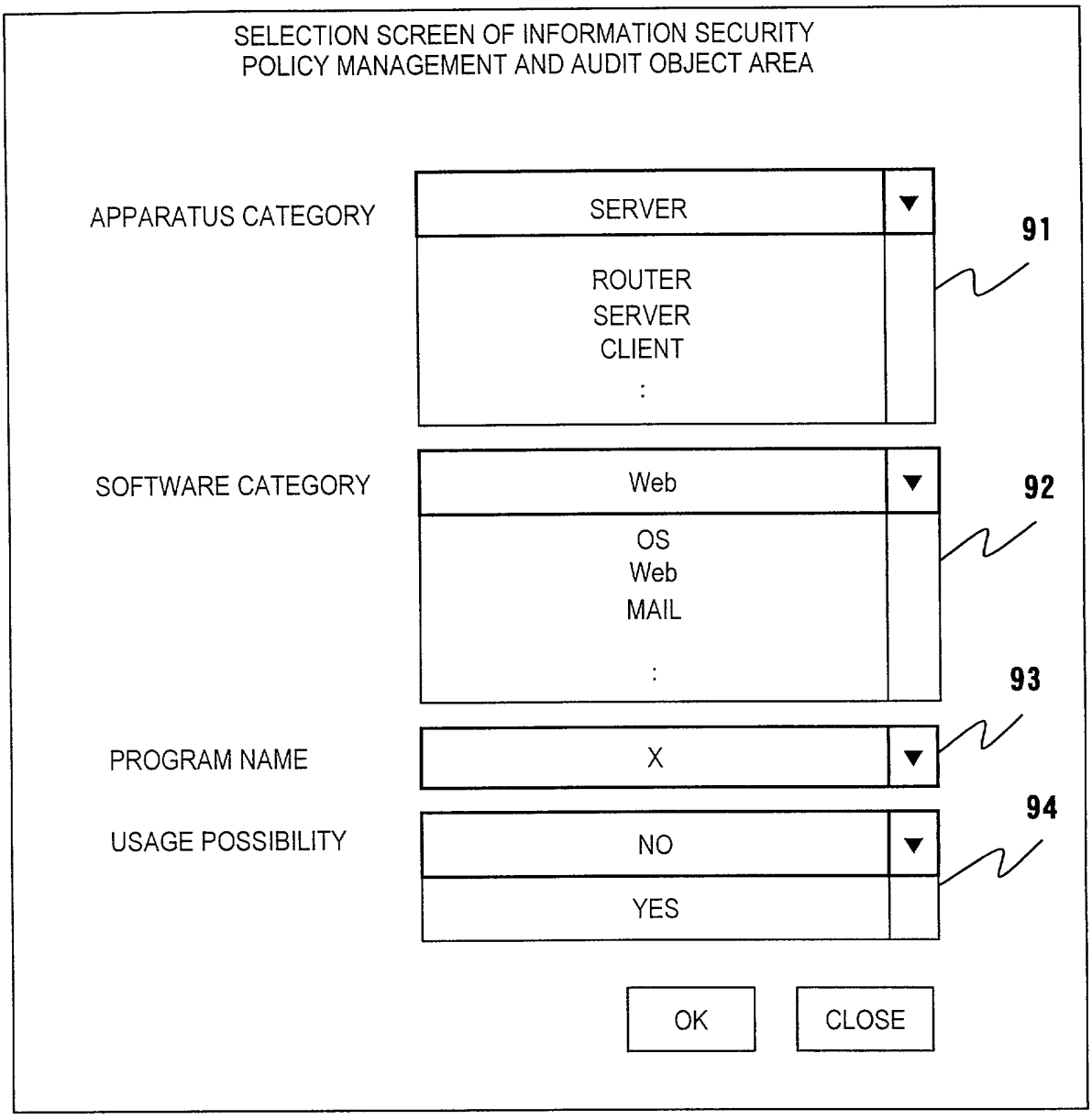
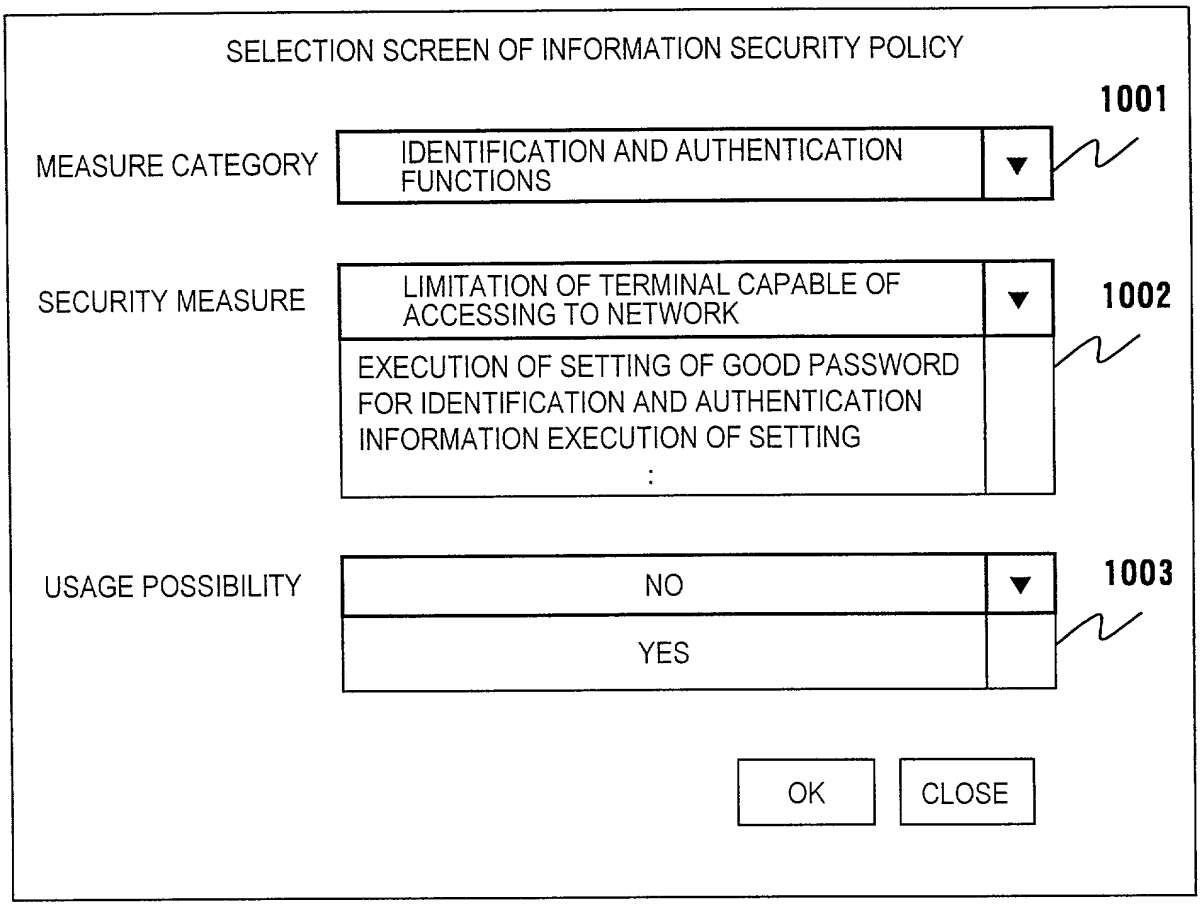

SELECTION SCREEN OF INFORMATION SECURITY POLICY MANAGEMENT AND AUDIT OBJECT AREA
APPARATUS CATEGORY
SERVER
ROUTER
SERVER
CLIENT
:
91
SOFTWARE CATEGORY
Web
OS
Web
MAIL
:
92
93
PROGRAM NAME
X
USAGE POSSIBILITY
NO
YES
94
OK
CLOSE

FIG.9



0576742 05/26/04

FIG.10

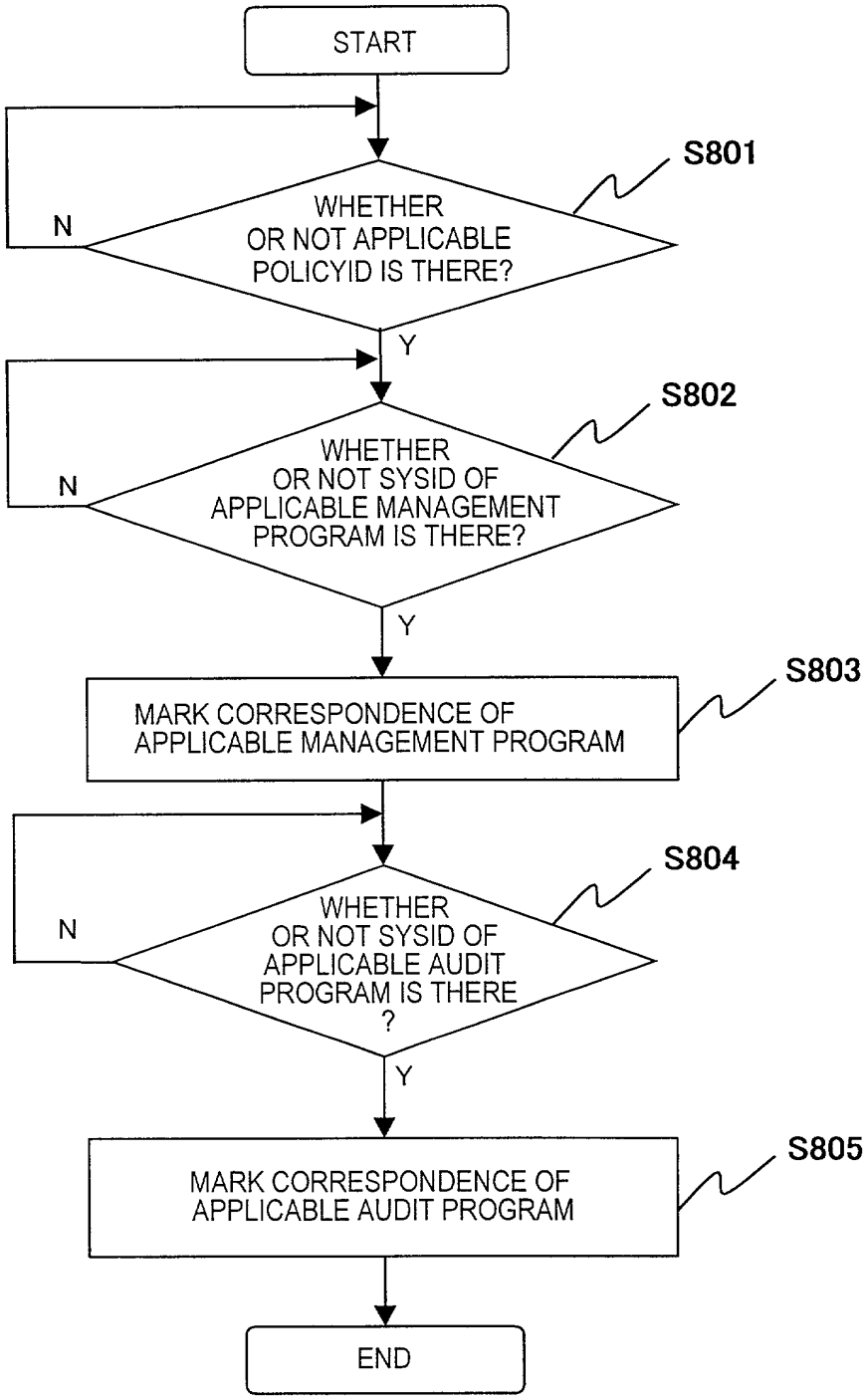

START
S801
WHETHER OR NOT APPLICABLE POLICYID IS THERE?
N
Y
S802
WHETHER OR NOT SYSID OF APPLICABLE MANAGEMENT PROGRAM IS THERE?
N
Y
S803
MARK CORRESPONDENCE OF APPLICABLE MANAGEMENT PROGRAM
S804
WHETHER OR NOT SYSID OF APPLICABLE AUDIT PROGRAM IS THERE ?
N
Y
S805
MARK CORRESPONDENCE OF APPLICABLE AUDIT PROGRAM
END

FIG.11

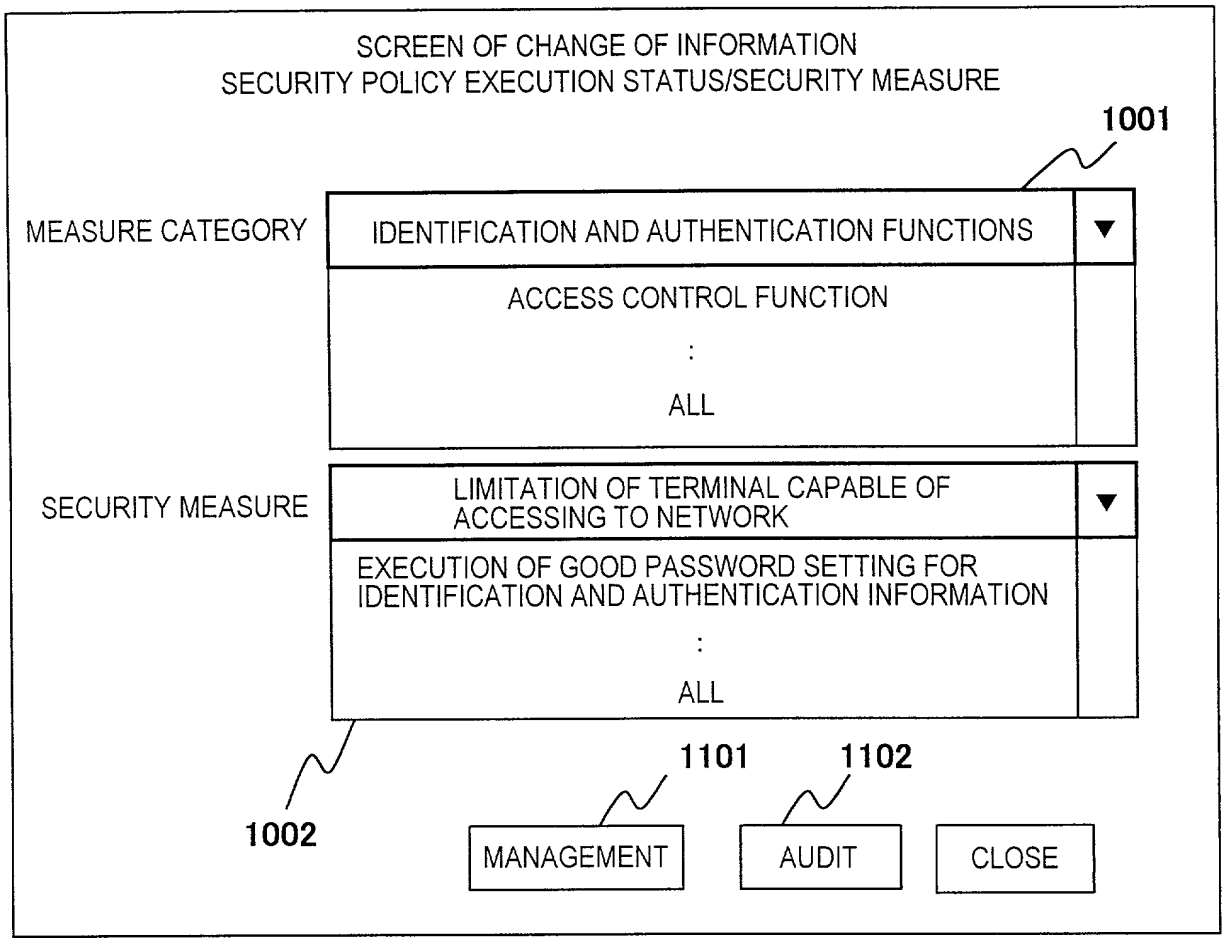
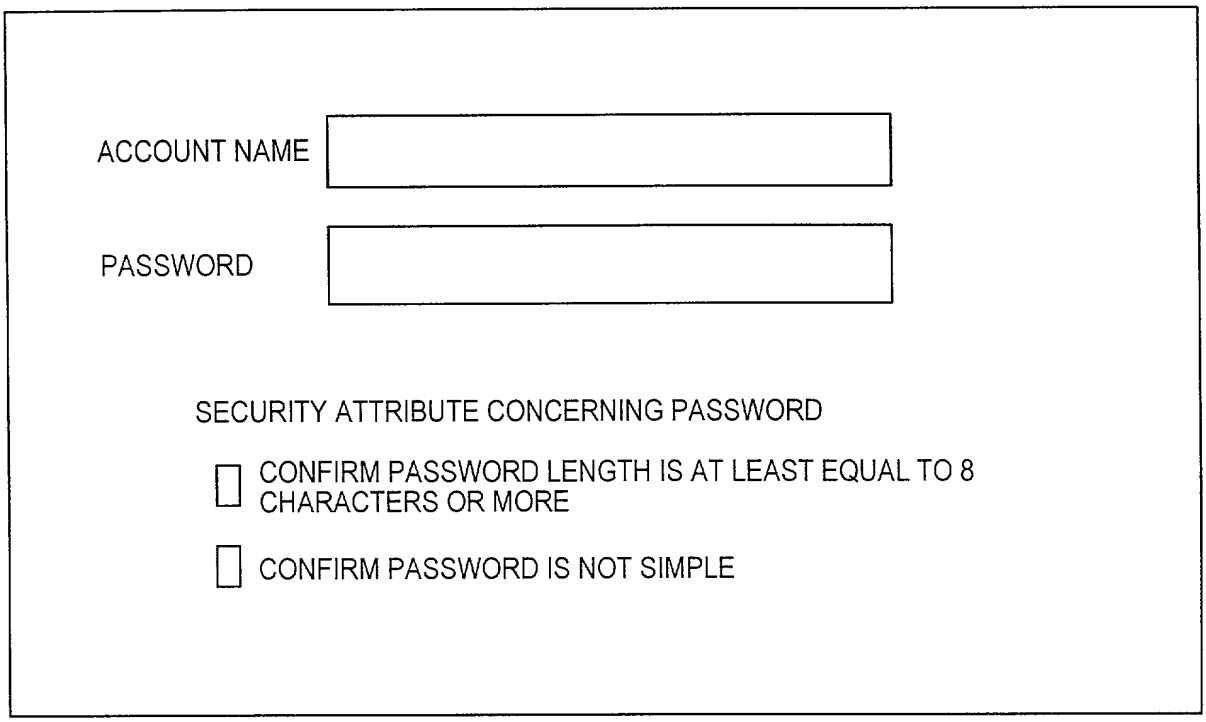

SCREEN OF CHANGE OF INFORMATION
SECURITY POLICY EXECUTION STATUS/SECURITY MEASURE
1001
MEASURE CATEGORY
IDENTIFICATION AND AUTHENTICATION FUNCTIONS
ACCESS CONTROL FUNCTION
:
ALL
SECURITY MEASURE
LIMITATION OF TERMINAL CAPABLE OF ACCESSING TO NETWORK
EXECUTION OF GOOD PASSWORD SETTING FOR IDENTIFICATION AND AUTHENTICATION INFORMATION
:
ALL
1002
1101
1102
MANAGEMENT
AUDIT
CLOSE

FIG.12



09754745 - 051801

FIG.13

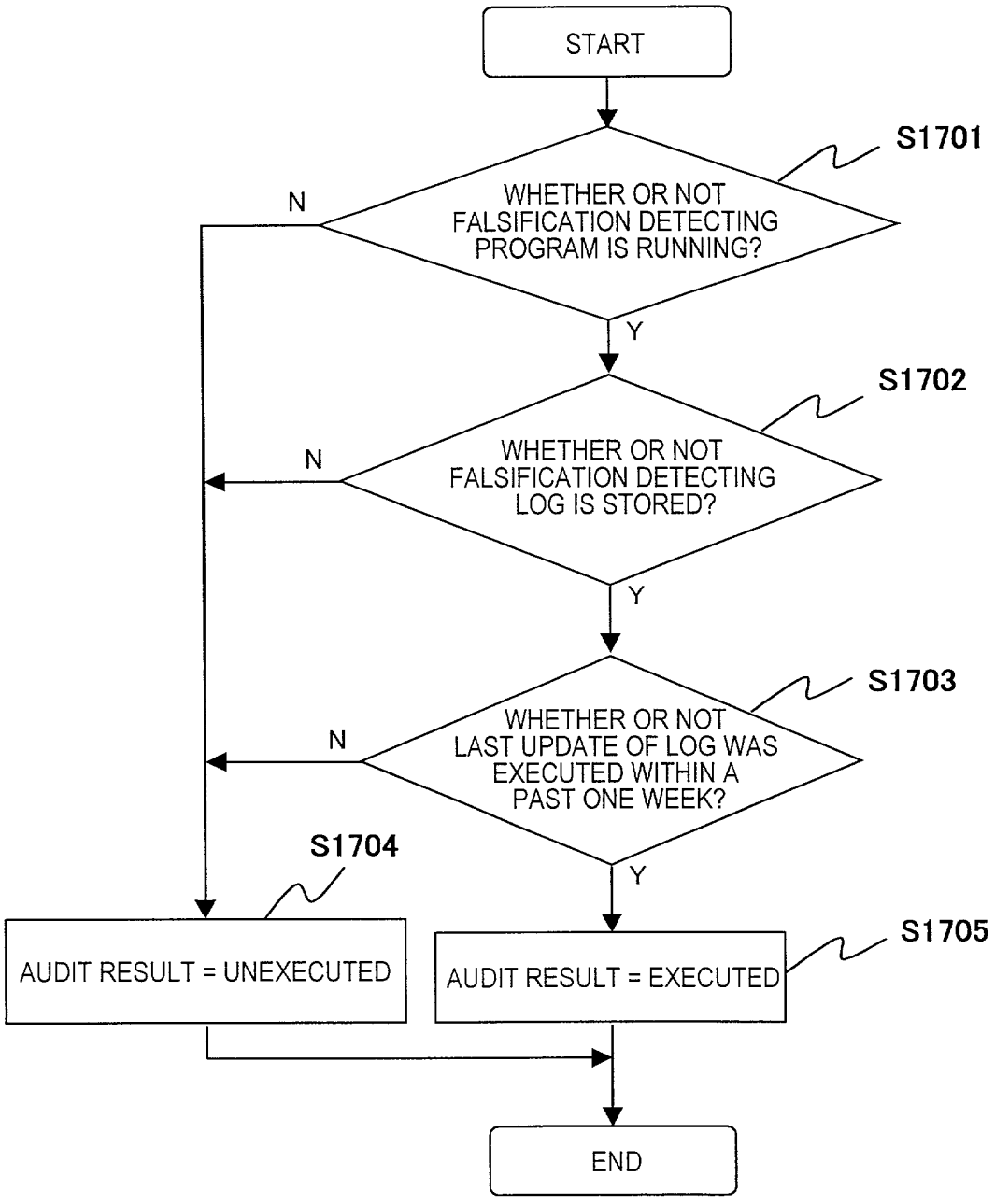

START
S1701
WHETHER OR NOT FALSIFICATION DETECTING PROGRAM IS RUNNING?
N
Y
S1702
WHETHER OR NOT FALSIFICATION DETECTING LOG IS STORED?
N
Y
S1703
WHETHER OR NOT LAST UPDATE OF LOG WAS EXECUTED WITHIN A PAST ONE WEEK?
N
Y
S1704
AUDIT RESULT = UNEXECUTED
S1705
AUDIT RESULT = EXECUTED
END

FIG.14

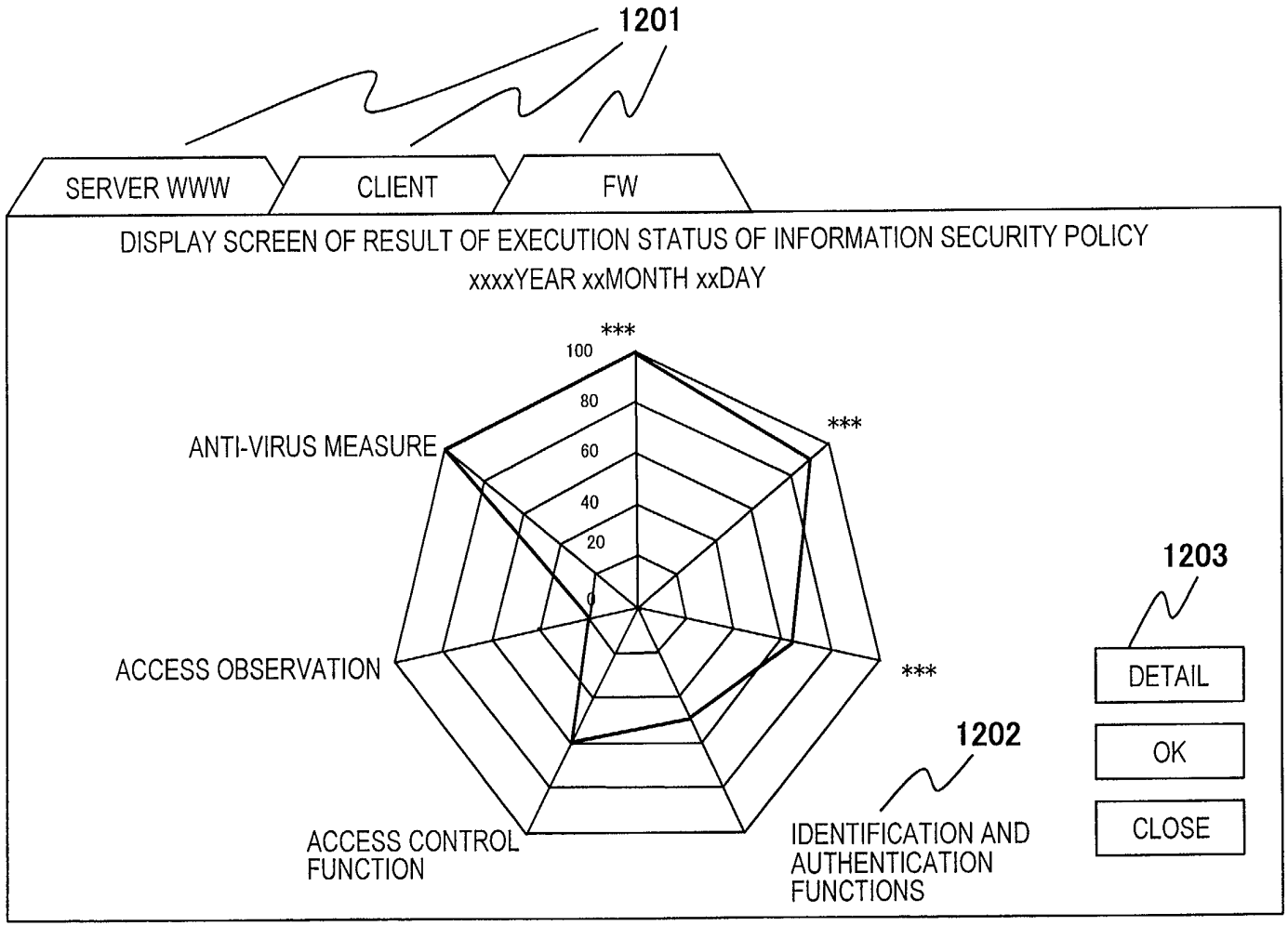

1201
SERVER WWW
CLIENT
FW
DISPLAY SCREEN OF RESULT OF EXECUTION STATUS OF INFORMATION SECURITY POLICY
xxxxYEAR xxMONTH xxDAY
***
100
80
60
40
20
0
***
ANTI-VIRUS MEASURE
ACCESS OBSERVATION
***
ACCESS CONTROL FUNCTION
IDENTIFICATION AND AUTHENTICATION FUNCTIONS
1202
1203
DETAIL
OK
CLOSE

FIG.15

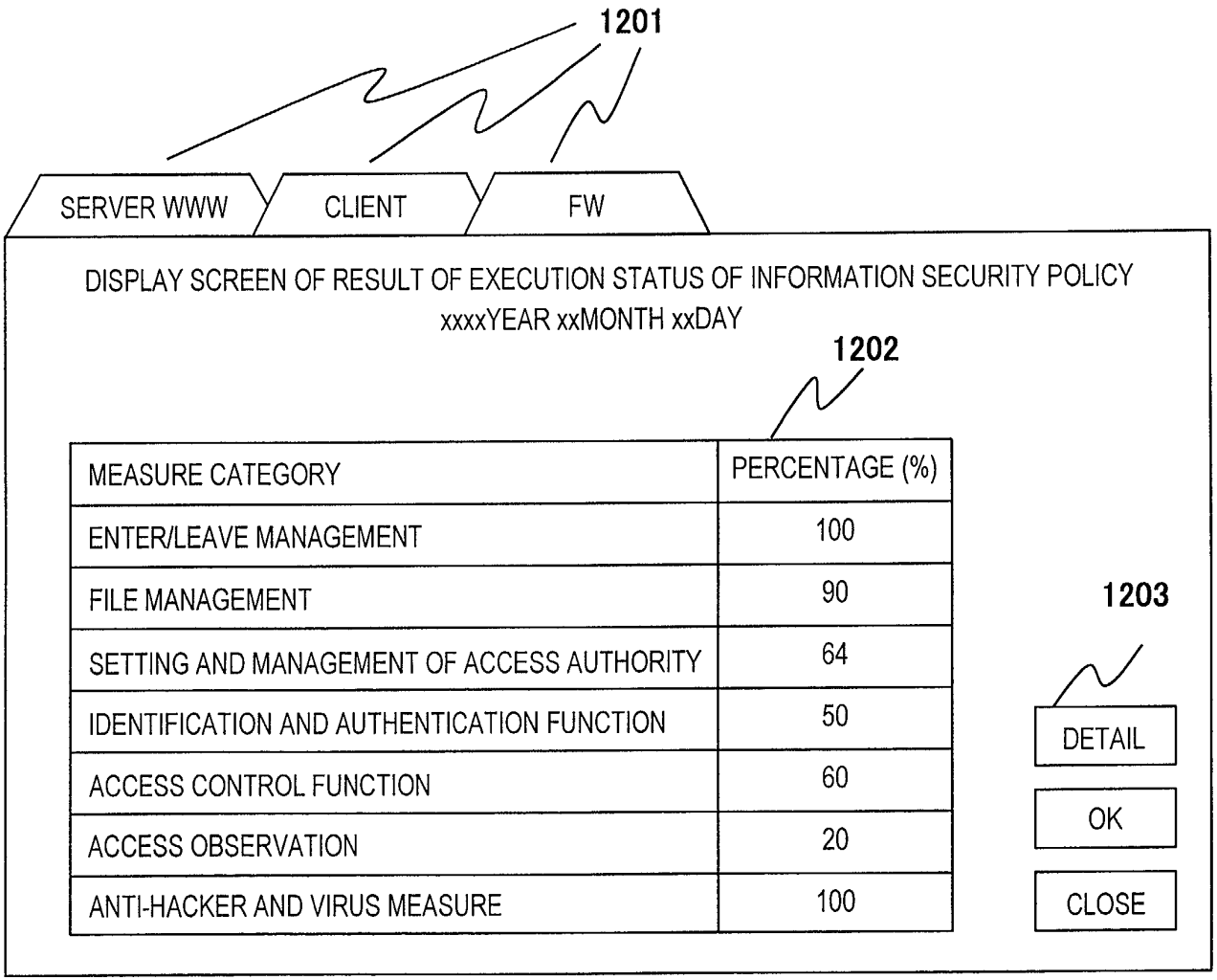
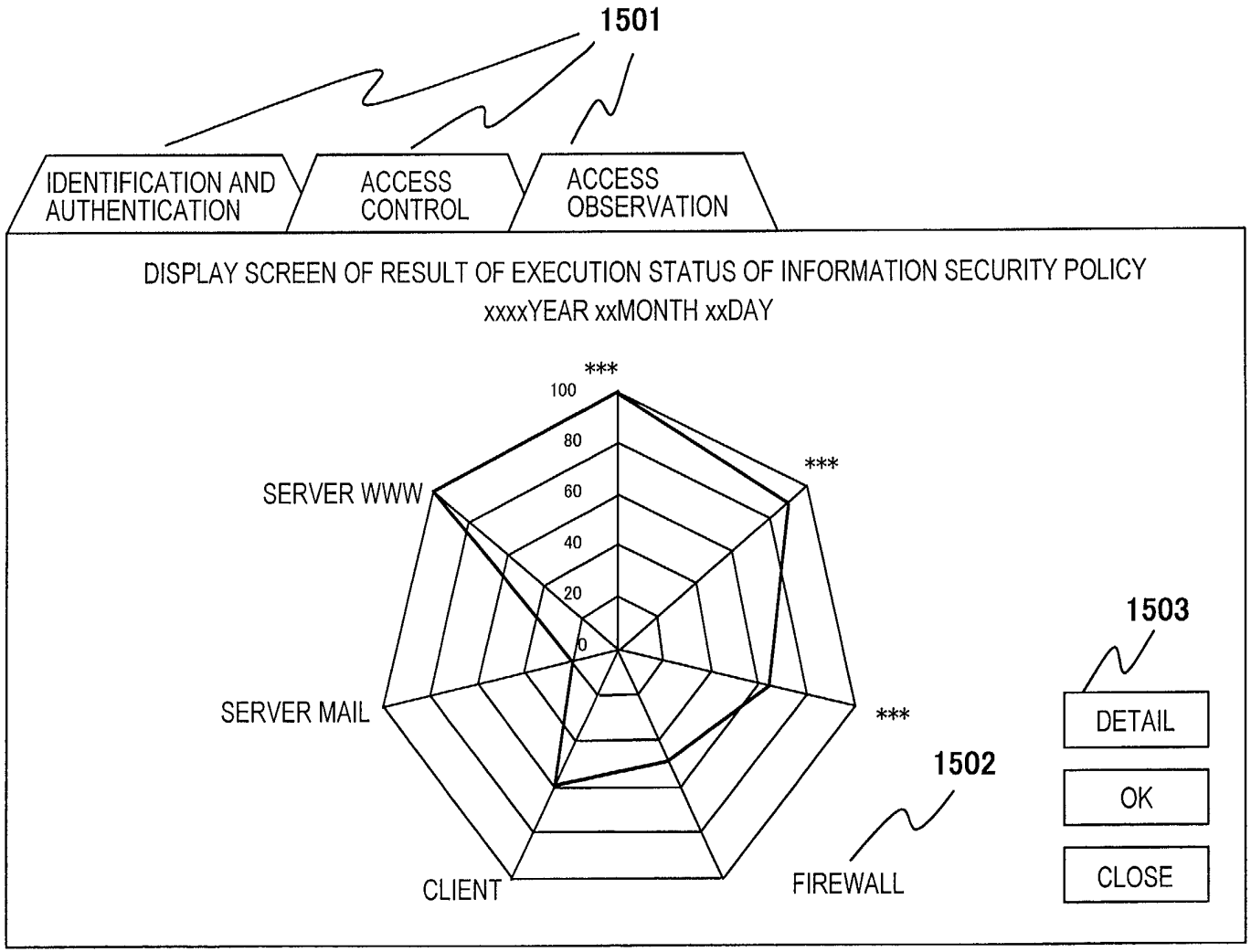

1201
SERVER WWW
CLIENT
FW
DISPLAY SCREEN OF RESULT OF EXECUTION STATUS OF INFORMATION SECURITY POLICY
xxxxYEAR xxMONTH xxDAY
1202
MEASURE CATEGORY
PERCENTAGE (%)
ENTER/LEAVE MANAGEMENT
100
FILE MANAGEMENT
90
SETTING AND MANAGEMENT OF ACCESS AUTHORITY
64
IDENTIFICATION AND AUTHENTICATION FUNCTION
50
ACCESS CONTROL FUNCTION
60
ACCESS OBSERVATION
20
ANTI-HACKER AND VIRUS MEASURE
100
1203
DETAIL
OK
CLOSE

FIG.16


1501
IDENTIFICATION AND AUTHENTICATION
ACCESS CONTROL
ACCESS OBSERVATION
DISPLAY SCREEN OF RESULT OF EXECUTION STATUS OF INFORMATION SECURITY POLICY
xxxxYEAR xxMONTH xxDAY
***
100
80
60
40
20
0
***
***
***
SERVER WWW
SERVER MAIL
CLIENT
FIREWALL
1502
1503
DETAIL
OK
CLOSE

T08150" 2007/09/26

FIG.17

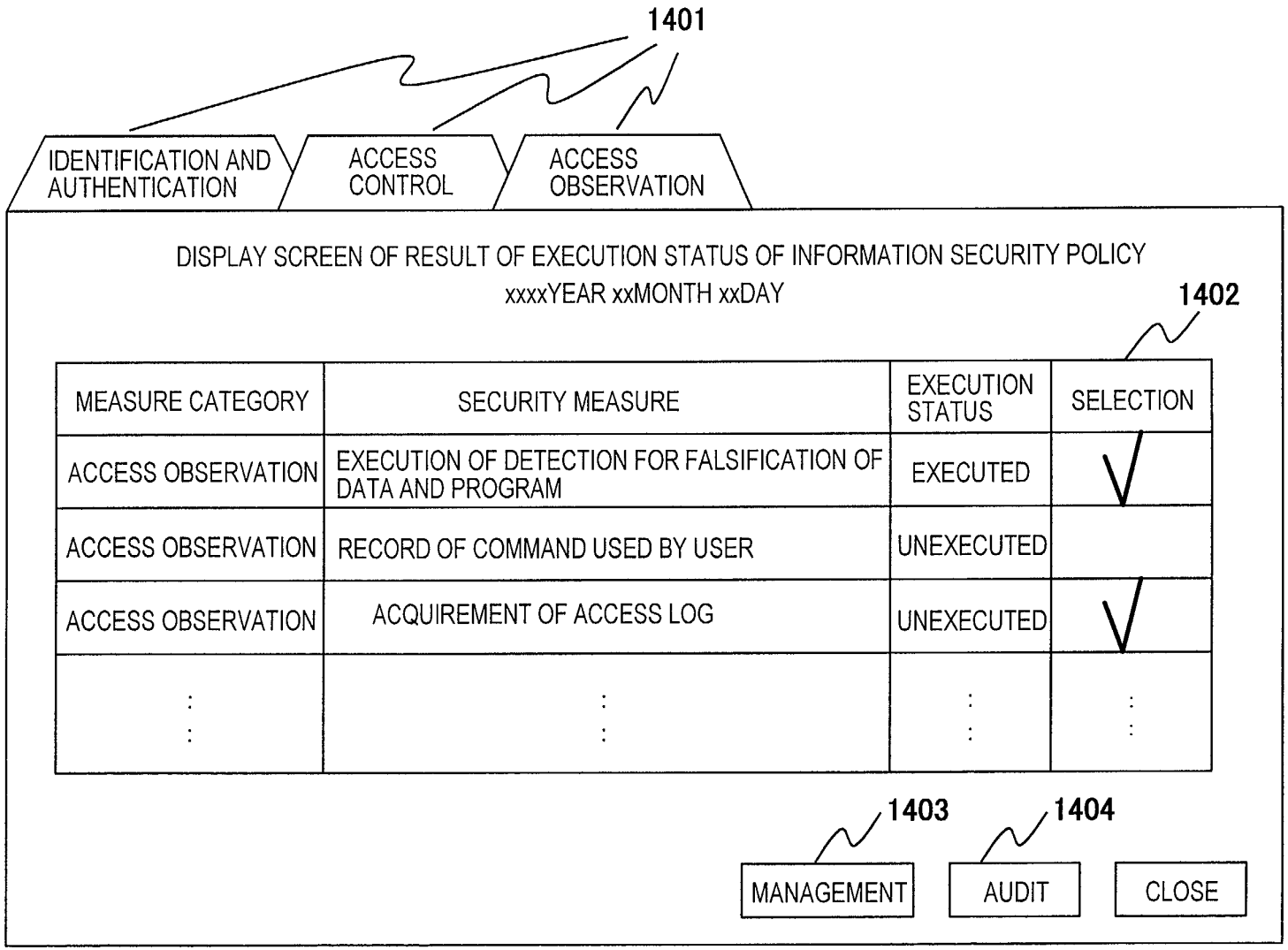


FIG.18

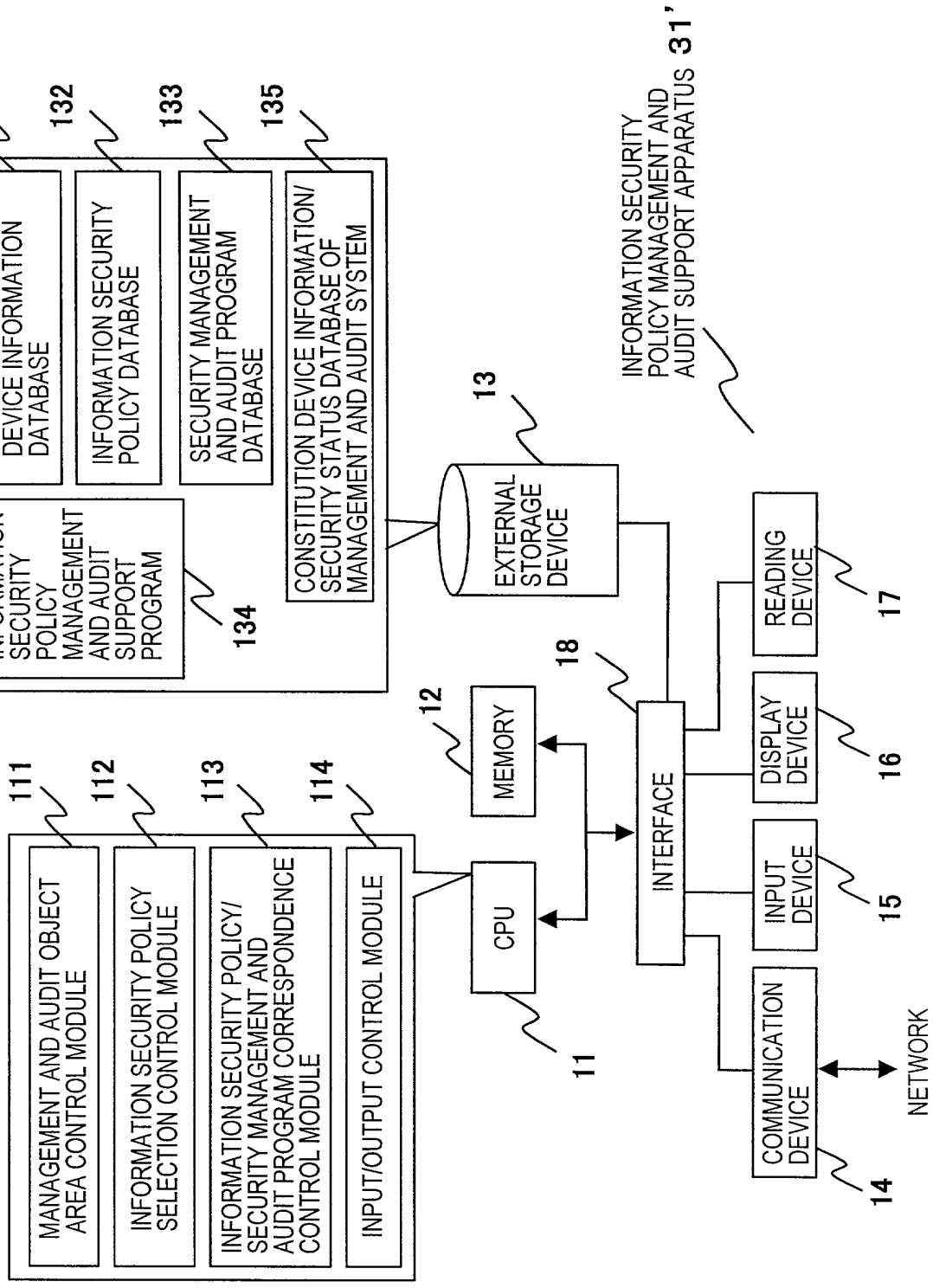

131
SYSTEM CONSTITUTION DEVICE INFORMATION DATABASE
132
INFORMATION SECURITY POLICY DATABASE
133
SECURITY MANAGEMENT AND AUDIT PROGRAM DATABASE
135
CONSTITUTION DEVICE INFORMATION/ SECURITY STATUS DATABASE OF MANAGEMENT AND AUDIT SYSTEM
INFORMATION SECURITY POLICY MANAGEMENT AND AUDIT SUPPORT PROGRAM
134
13
EXTERNAL STORAGE DEVICE
INFORMATION SECURITY POLICY MANAGEMENT AND AUDIT SUPPORT APPARATUS 31'
111
MANAGEMENT AND AUDIT OBJECT AREA CONTROL MODULE
112
INFORMATION SECURITY POLICY SELECTION CONTROL MODULE
113
INFORMATION SECURITY POLICY/ SECURITY MANAGEMENT AND AUDIT PROGRAM CORRESPONDENCE CONTROL MODULE
114
INPUT/OUTPUT CONTROL MODULE
12
MEMORY
18
INTERFACE
READING DEVICE
17
DISPLAY DEVICE
16
INPUT DEVICE
15
CPU
11
COMMUNICATION DEVICE
14
NETWORK

FIG.19

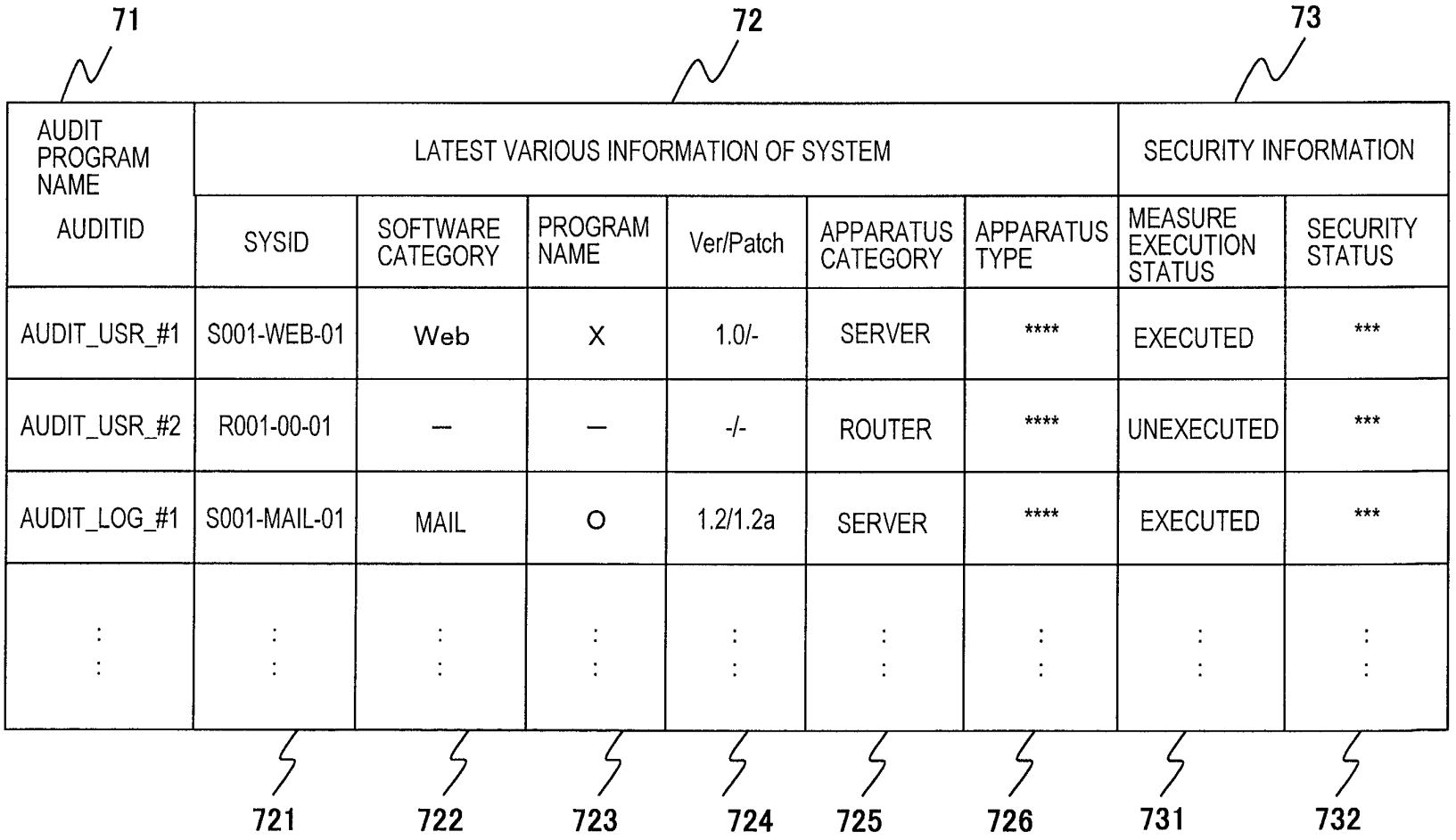

71
72
73
AUDIT PROGRAM NAME
AUDITID
LATEST VARIOUS INFORMATION OF SYSTEM
SECURITY INFORMATION
SYSID
SOFTWARE CATEGORY
PROGRAM NAME
Ver/Patch
APPARATUS CATEGORY
APPARATUS TYPE
MEASURE EXECUTION STATUS
SECURITY STATUS
AUDIT_USR_#1
S001-WEB-01
Web
X
1.0/-
SERVER
****
EXECUTED
***
AUDIT_USR_#2
R001-00-01
—
—
-/-
ROUTER
****
UNEXECUTED
***
AUDIT_LOG_#1
S001-MAIL-01
MAIL
O
1.2/1.2a
SERVER
****
EXECUTED
***
721
722
723
724
725
726
731
732

FIG.20

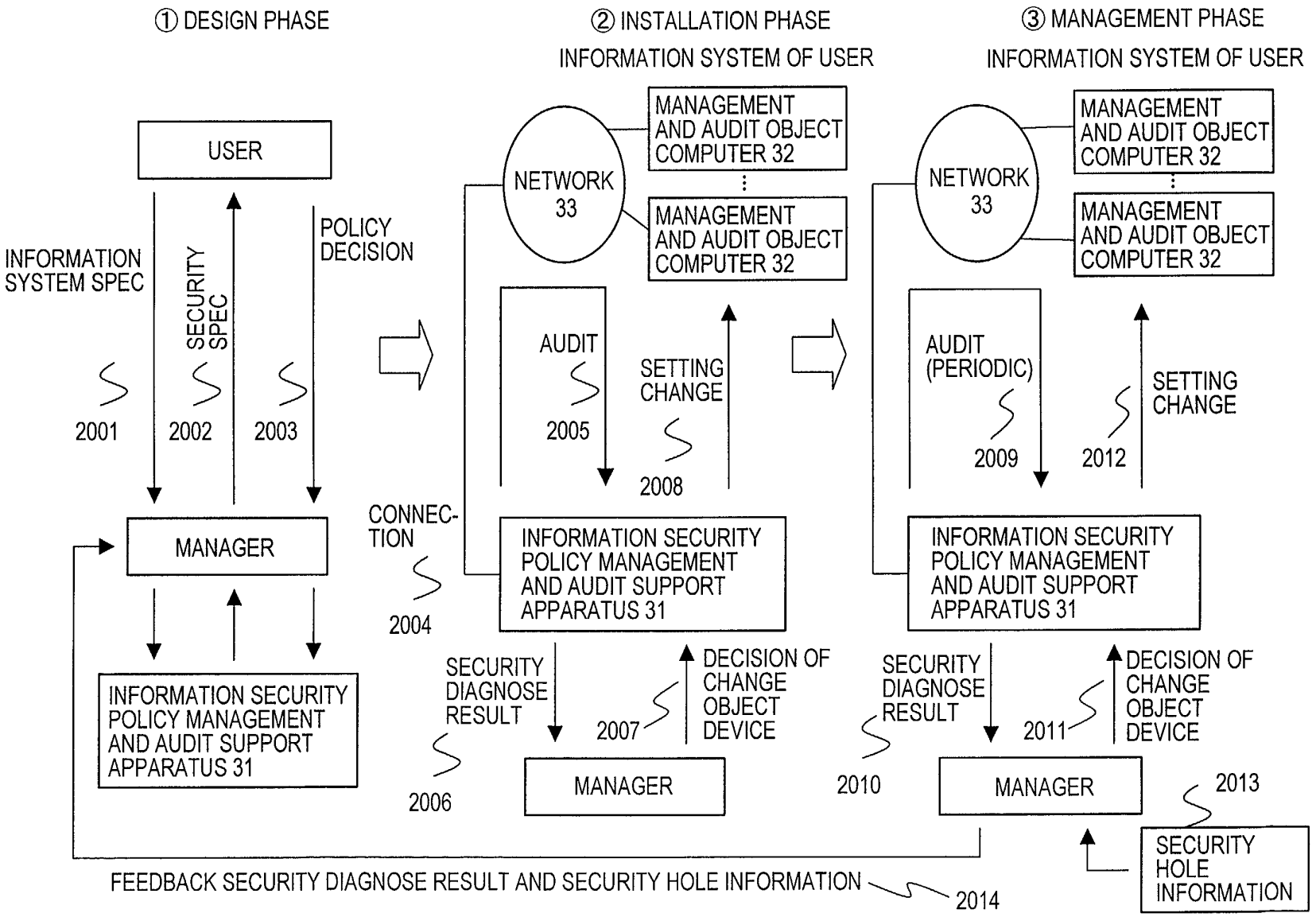

① DESIGN PHASE
② INSTALLATION PHASE
INFORMATION SYSTEM OF USER
③ MANAGEMENT PHASE
INFORMATION SYSTEM OF USER
USER
INFORMATION SYSTEM SPEC
SECURITY SPEC
POLICY DECISION
2001
2002
2003
MANAGER
INFORMATION SECURITY POLICY MANAGEMENT AND AUDIT SUPPORT APPARATUS 31
NETWORK 33
MANAGEMENT AND AUDIT OBJECT COMPUTER 32
MANAGEMENT AND AUDIT OBJECT COMPUTER 32
AUDIT
2005
SETTING CHANGE
2008
CONNEC-TION
2004
INFORMATION SECURITY POLICY MANAGEMENT AND AUDIT SUPPORT APPARATUS 31
SECURITY DIAGNOSE RESULT
2006
2007
DECISION OF CHANGE OBJECT DEVICE
MANAGER
NETWORK 33
MANAGEMENT AND AUDIT OBJECT COMPUTER 32
MANAGEMENT AND AUDIT OBJECT COMPUTER 32
AUDIT (PERIODIC)
2009
SETTING CHANGE
2012
INFORMATION SECURITY POLICY MANAGEMENT AND AUDIT SUPPORT APPARATUS 31
SECURITY DIAGNOSE RESULT
2010
2011
DECISION OF CHANGE OBJECT DEVICE
MANAGER
2013
SECURITY HOLE INFORMATION
FEEDBACK SECURITY DIAGNOSE RESULT AND SECURITY HOLE INFORMATION
2014

FIG.21

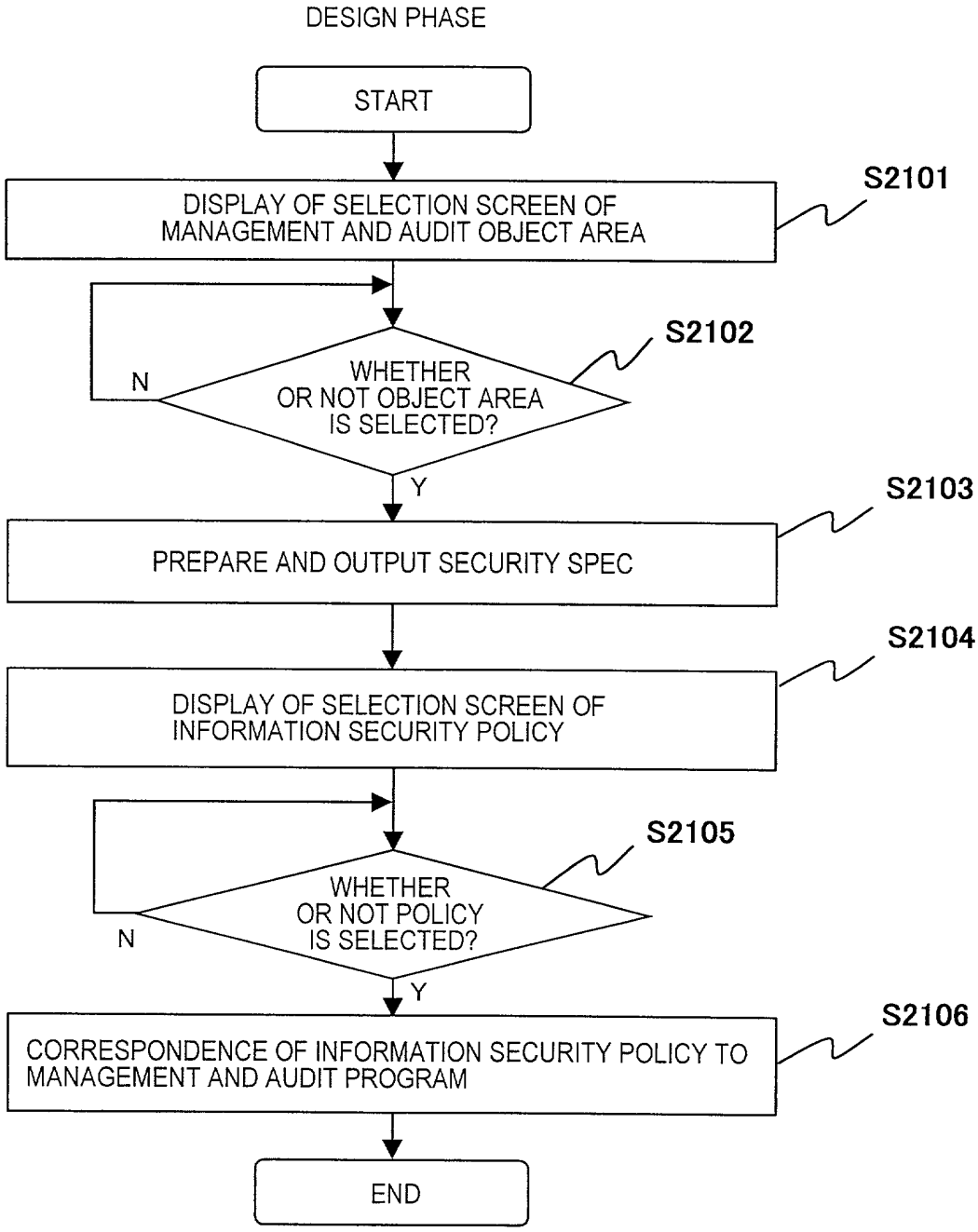

DESIGN PHASE
START
DISPLAY OF SELECTION SCREEN OF MANAGEMENT AND AUDIT OBJECT AREA
S2101
WHETHER OR NOT OBJECT AREA IS SELECTED?
S2102
N
Y
PREPARE AND OUTPUT SECURITY SPEC
S2103
DISPLAY OF SELECTION SCREEN OF INFORMATION SECURITY POLICY
S2104
WHETHER OR NOT POLICY IS SELECTED?
S2105
N
Y
CORRESPONDENCE OF INFORMATION SECURITY POLICY TO MANAGEMENT AND AUDIT PROGRAM
S2106
END

FIG.22

SECURITY SPECIFICATION

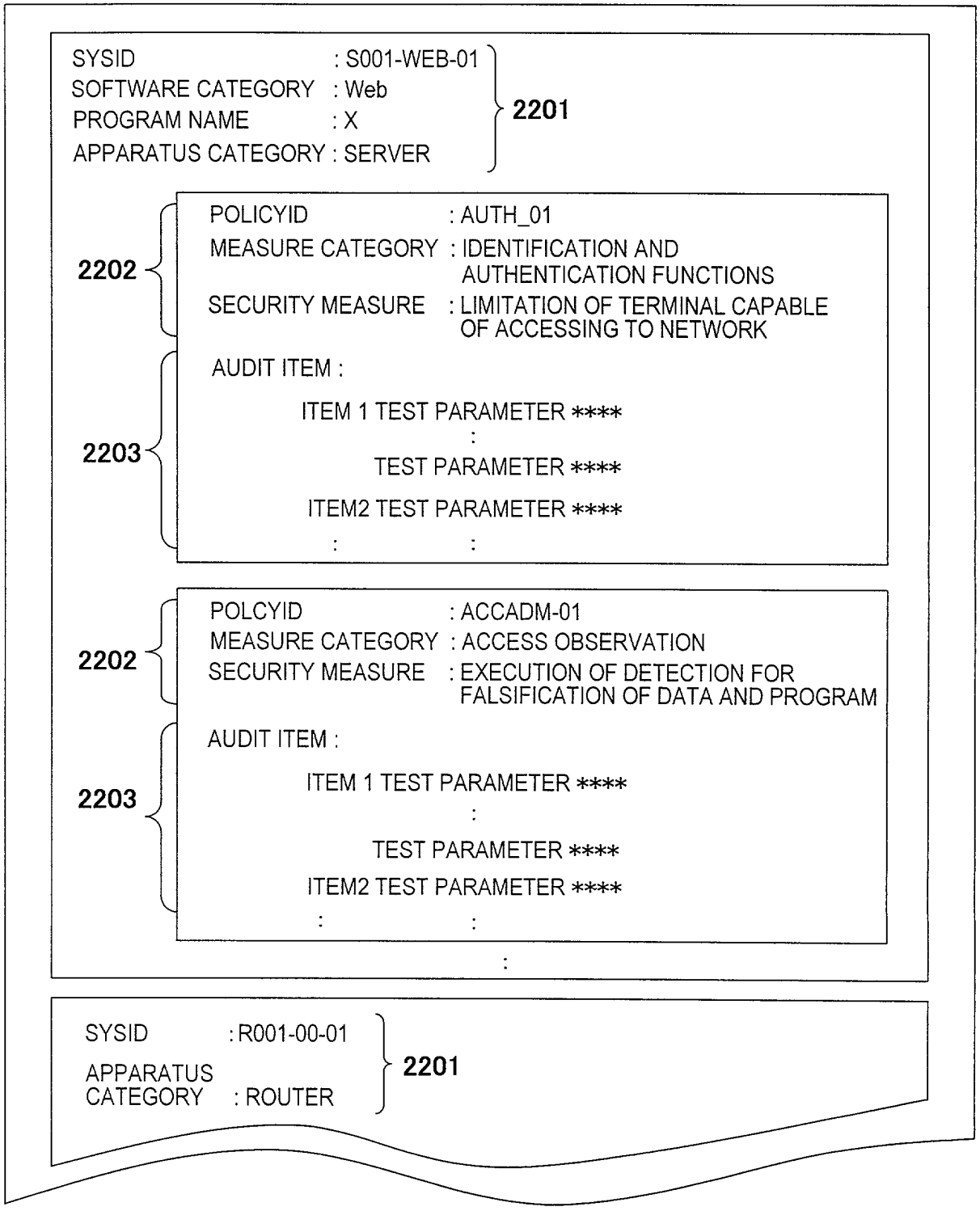


FIG.23

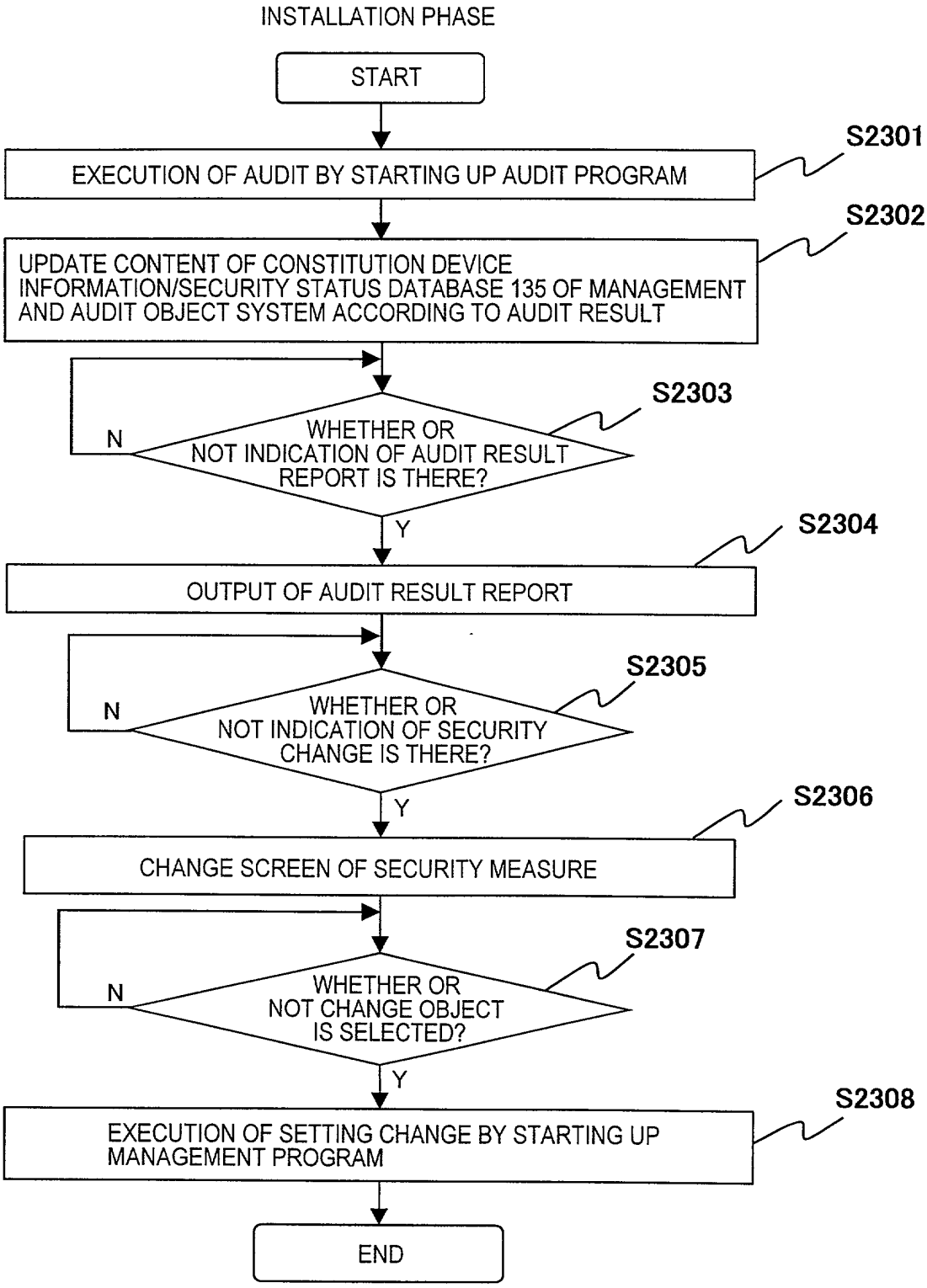

INSTALLATION PHASE
START
S2301
EXECUTION OF AUDIT BY STARTING UP AUDIT PROGRAM
S2302
UPDATE CONTENT OF CONSTITUTION DEVICE INFORMATION/SECURITY STATUS DATABASE 135 OF MANAGEMENT AND AUDIT OBJECT SYSTEM ACCORDING TO AUDIT RESULT
S2303
WHETHER OR NOT INDICATION OF AUDIT RESULT REPORT IS THERE?
N
Y
S2304
OUTPUT OF AUDIT RESULT REPORT
S2305
WHETHER OR NOT INDICATION OF SECURITY CHANGE IS THERE?
N
Y
S2306
CHANGE SCREEN OF SECURITY MEASURE
S2307
WHETHER OR NOT CHANGE OBJECT IS SELECTED?
N
Y
S2308
EXECUTION OF SETTING CHANGE BY STARTING UP MANAGEMENT PROGRAM
END

FIG.24

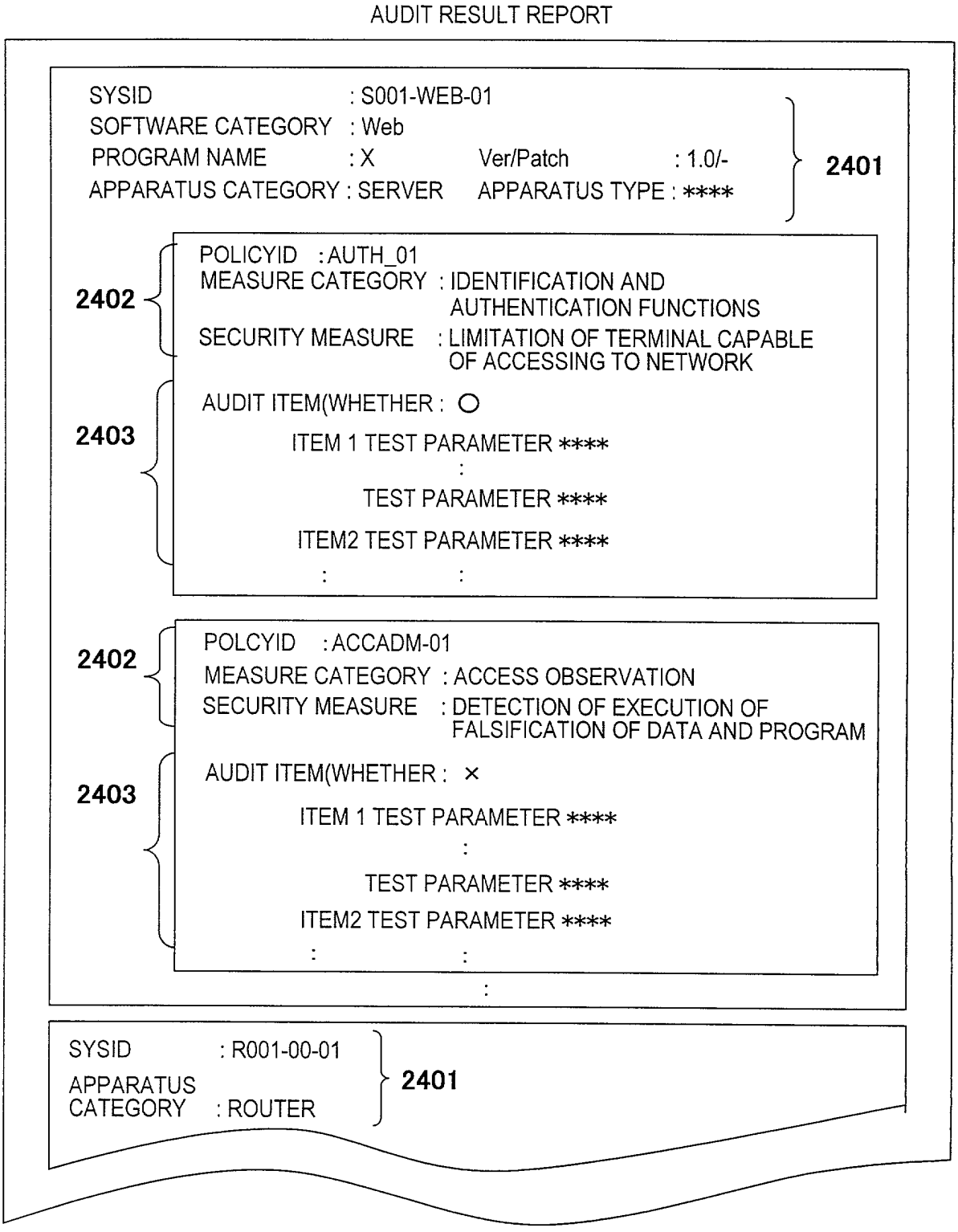

AUDIT RESULT REPORT
SYSID : S001-WEB-01
SOFTWARE CATEGORY : Web
PROGRAM NAME : X
Ver/Patch : 1.0/-
APPARATUS CATEGORY : SERVER
APPARATUS TYPE : ****
2401
2402
POLICYID : AUTH_01
MEASURE CATEGORY : IDENTIFICATION AND AUTHENTICATION FUNCTIONS
SECURITY MEASURE : LIMITATION OF TERMINAL CAPABLE OF ACCESSING TO NETWORK
2403
AUDIT ITEM(WHETHER : ○
ITEM 1 TEST PARAMETER ****
:
TEST PARAMETER ****
ITEM2 TEST PARAMETER ****
: :
2402
POLCYID : ACCADM-01
MEASURE CATEGORY : ACCESS OBSERVATION
SECURITY MEASURE : DETECTION OF EXECUTION OF FALSIFICATION OF DATA AND PROGRAM
2403
AUDIT ITEM(WHETHER : ×
ITEM 1 TEST PARAMETER ****
:
TEST PARAMETER ****
ITEM2 TEST PARAMETER ****
: :
:
SYSID : R001-00-01
APPARATUS CATEGORY : ROUTER
2401

FIG.25

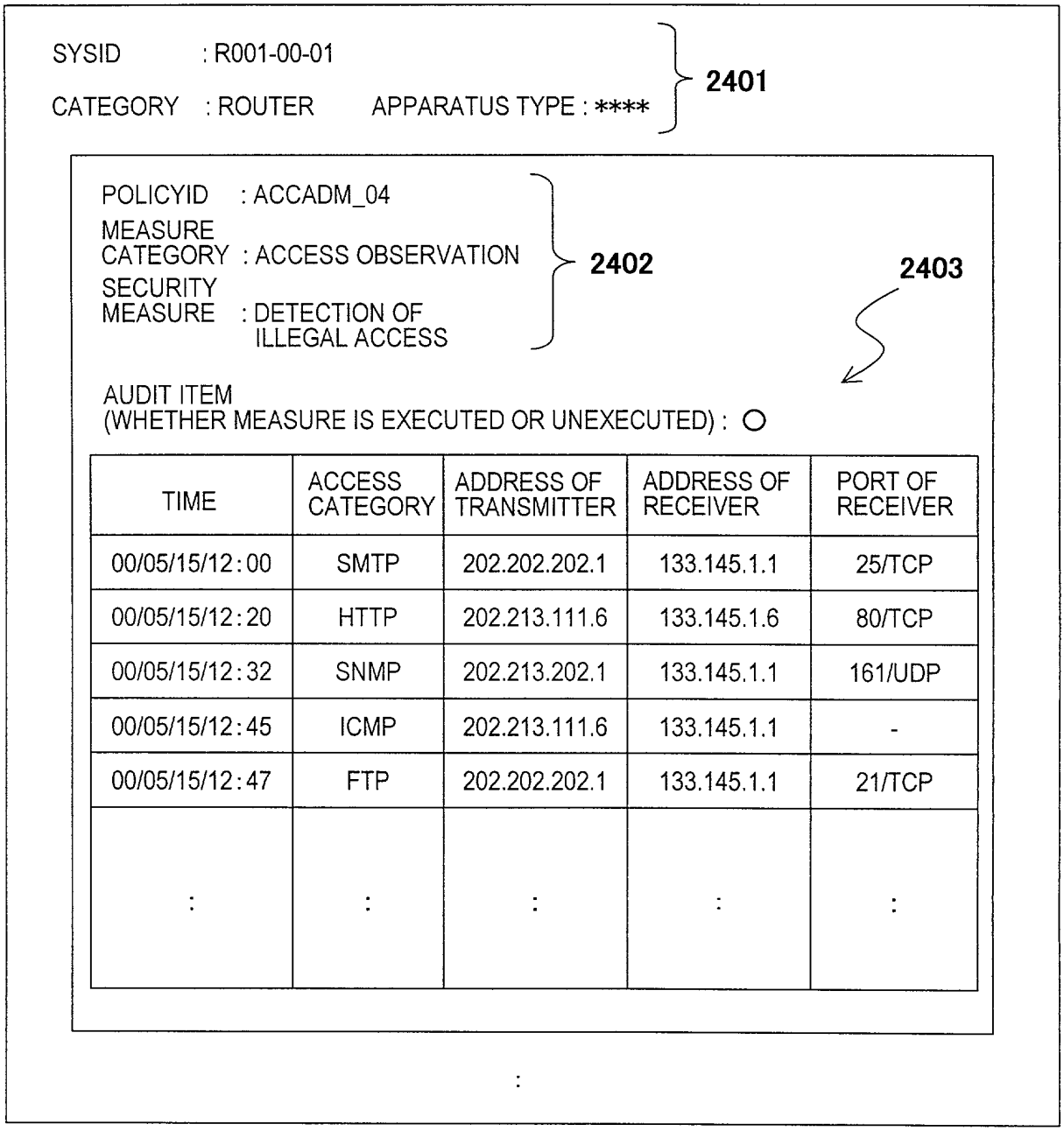
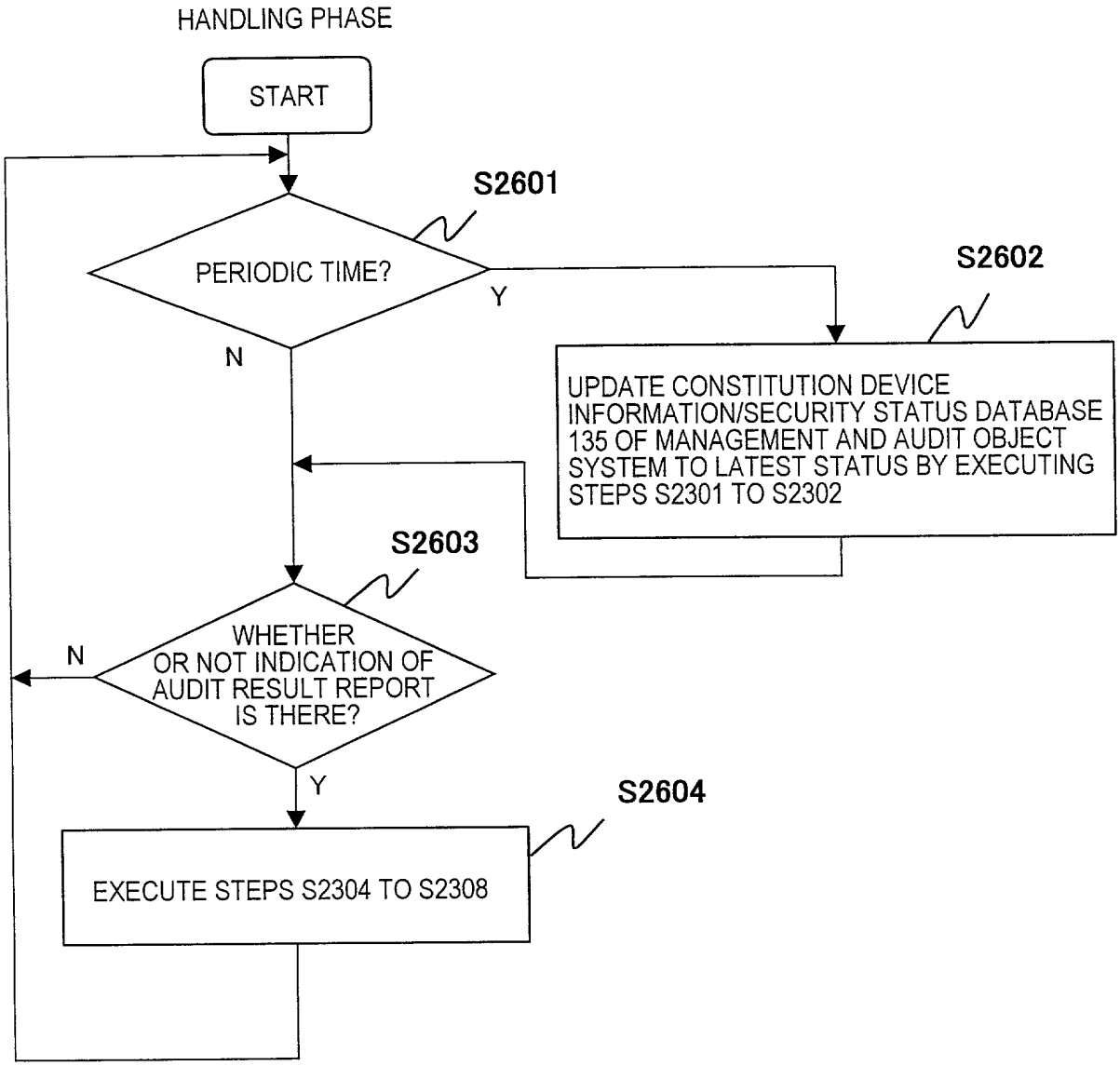

SYSID : R001-00-01
CATEGORY : ROUTER APPARATUS TYPE : ****
2401
POLICYID : ACCADM_04
MEASURE CATEGORY : ACCESS OBSERVATION
SECURITY MEASURE : DETECTION OF ILLEGAL ACCESS
2402
2403
AUDIT ITEM
(WHETHER MEASURE IS EXECUTED OR UNEXECUTED) : ○
TIME
ACCESS CATEGORY
ADDRESS OF TRANSMITTER
ADDRESS OF RECEIVER
PORT OF RECEIVER
00/05/15/12:00 SMTP 202.202.202.1 133.145.1.1 25/TCP
00/05/15/12:20 HTTP 202.213.111.6 133.145.1.6 80/TCP
00/05/15/12:32 SNMP 202.213.202.1 133.145.1.1 161/UDP
00/05/15/12:45 ICMP 202.213.111.6 133.145.1.1 -
00/05/15/12:47 FTP 202.202.202.1 133.145.1.1 21/TCP

FIG.26



09251962-051801